REMARKS

Claims 1-47 are in the application. Claims 2, 10, 17 and 20 are corrected. Claims 32 and 42 are amended to overcome the 35 USC § 112 rejections. Claims 46 and 47 are added to better protect the invention without introducing new matter. A listing of the claims is provided as required by the new USPTO amendment practice per 37 CFR 1.121.

This responsive amendment follows the relevant paragraphs of the office action to enable ease of following and understanding.

The office action states, "Drawings

1. Figures 1-3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

In response applicant respectfully states that the drawings are corrected and Figures 1-3 are designated as prior art. A new set of formal drawings are included herewith.

The office action further states, " Specification

2. The abstract of the disclosure is objected to because of the following informalities: Abstract contains more than 150 words. Correction is required.

3. Applicant is reminded of the proper language and format for an abstract of the disclosure. The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details. The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

In response applicant respectfully states that the abstract has been amended to have 150 words or less.

The office action states, "
4. The arrangement of the disclosed application does not conform with 37 CFR 1.77(b).

Section headings are boldfaced throughout the disclosed specification. Section headings should not be underlined and/or boldfaced. Appropriate corrections are required.

In response applicant respectfully states that the boldface was removed from the section headings and provided herein in the amendment to the specification.

The office action further states, " Claim Objections

5. Claim 42 is objected to because of the following informalities: Claim 42 does not end in a period. Each claim should begin with a capital letter and end with a period. Appropriate correction is required.

In response applicant respectfully states that claim 42 is amended herein to end with a period, to correct the informality.

The office action further states, " Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112: The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 32 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In lines 10-11 it is unclear how "dividing said cipher-text message into a plurality of cipher-text blocks" would "form an encryption of said plain text message". The specification does not show this in such a way as to enable "dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of said plan-text message". Appropriate correction is required.

In response applicant respectfully states that claim 32 is amended to delete the words. "to form an encryption of said plain-text message; so that line 10-11 read, "dividing said cipher-text message into a plurality of cipher-text blocks". This overcomes the *rejection under 35 U.S.C. 112, first paragraph*, and makes claim 32 allowable.

The office action further states, "Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action: (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of *this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

9. Claims 1-6,8,10-12,22-23,26,28,30,33,35,37,39, and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No.1 063811 A 1) in view of Takahashi (U.S. patent No. 5,570,307).

As to Claim 1, Furuya et al. teaches a method for encrypting a plain-text message (see page 2, lines 1-3), the method comprising: further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 7, line 54 through page 8, line 10); dividing said plain-text message into a plurality of plain-text blocks (see figure 15); encrypting said plain-text blocks to form a plurality of cipher-text blocks (see page 5, lines 31-38); combining said plurality of plain-text blocks into at least one check sum (see figure 6); and employing said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks (see page 5, lines 39-43). Furuya et al. does not teach generating a first random number; and transforming said first random number into a first pseudo random number. Takahashi teaches generating a first random number (see column 3, lines 4~13); and transforming said first random number into a first pseudo random number (see column 3, lines 14-29).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include generating a first random number; and transforming said first random number into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Takahashi because generating a first random number; and transforming said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20).

In response applicant respectfully states that although Furuya et al. with Takahashi may teach generating pseudo random numbers for the process of encryption, they do not teach generating pairwise differentially uniform numbers and using such numbers in the encryption process. All the claims in the present invention have an element using pairwise differentially uniform numbers in the encryption process, as such numbers are more easily generated than general purpose pseudo random numbers. It is well known in prior art, that a sequence of n pairwise differentially uniform numbers, each of m bits, can be generated from a single number of m bits, by a single cheap operation like addition or multiplication in a Galois field. In contrast, a sequence of n general purpose pseudo random numbers can only be generated by cryptographic means like keystream generators, stream ciphers or other such cryptographic operations, which are generally an order of magnitude more costlier/inefficient to implement.

The embodiment, as described in the text, allows for the first time to encrypt and simultaneously provide integrity, with only about n cryptographic operations, when the data to be encrypted is n blocks. All previous schemes, including the one described in Furuya et al, require two times n cryptographic operations to achieve both encryption and integrity. Moreover, an embodiment described in the text employing the claimed invention, allows for all the n cryptographic operations to be performed in parallel, which is definitely not the case with the Furuya et al embodiment; as it uses stream ciphers which are inherently sequential.

The presently claimed invention achieves this efficiency, because of its use of pairwise differentially uniform numbers in a novel fashion, which as mentioned above, are reduced or almost free of cost to generate. Thus, even though the numbers used have a weaker property, we are able to show that they suffice to achieve the end goal of encryption with integrity.

> *The office action further states, "As to claim 2, Furuya et al. as modified, teaches wherein the step of encrypting said plain-text blocks includes employing the said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers (see Furuya et al., column 5, lines 31-38).*

In response applicant respectfully states that Furuya et al only teach generating a pseudo random number sequence and using it for encryption, whereas Claim 2 teaches using pair-wise differentially uniform random numbers, which are much weaker than general pseudo random numbers, and much easier to generate. Thus claim 2 is allowable over Furuya et al.

> *The office action further states, " As to claim 3, Furuya et al. as modified, teaches wherein the step of employing includes pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and combining each pair to form a plurality of output blocks (see Furuya et al., figure 15).*

In response applicant respectfully states that Furuya et al., does not teach employing pair-wise differentially uniform numbers as in claim 3, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 3 is allowable over Furuya et al.

> *The office action further states, "As to Claim 4, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., figure 15).*

In response applicant respectfully states that Claim 4 employs pair-wise differentially uniform numbers as in claim 3, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 4, which is dependent on Claim 3, is allowable over Furuya et al.

The office action further states, " As to claim 5, Furuya et al. as modified, teaches wherein the step of encrypting includes encrypting said first random number (see Furuya et al., figure 15, where "random number" can be read on "IV", see page 6, line 53).

In response applicant respectfully states that Claim 5 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 5, which is dependent on Claim 1, is allowable over Furuya et al.

The office action further states, " As to claim 6, Furuya et al. as modified, teaches wherein the step of encrypting includes encrypting said check sum (see Furuya et al., figure 6).

In response applicant respectfully states that Claim 6 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 6, which is dependent on Claim 1, is allowable over Furuya et al.

The office action further states, " As to claim 8, Furuya et al. as modified, teaches wherein the step of transforming said random number includes a non-cryptographic or linear operation (see Takahashi, column 3, lines 14-29).

In response applicant respectfully states that Claim 8 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 8, which is dependent on Claim 1, is allowable over Furuya et al. combined with Takahashi.

The office action further states, " As to claim 10, Furuya et al. as modified, teaches wherein the said set of pair- wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp (see Furuya et al., page 7, line 54 through page 8, line 10).

In response applicant respectfully states that although Furuya et al., may teach using operations in GFp, it does not teach generating or using numbers which are pairwise differentially uniform in GFp. Claim 10 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 10, which is dependent on Claim 1, is allowable over Furuya et al.

> *The office action further states, " As to claim 11, Furuya et al. as modified, teaches wherein the step of employing includes: pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and combining each pair to form a plurality of input blocks used in said step of encrypting (see Furuya et al., figure 15).*

In response applicant respectfully states that Furuya et al., does not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Claim 11 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 11, which is dependent on Claim 1, is allowable over Furuya et al.

> *The office action further states, " As to claim 12, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., figure 15).*

In response applicant respectfully states that Claim 12 employs pair-wise differentially uniform numbers as in claim 11, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 8, which is dependent on Claim 11, is allowable over Furuya et al.

> *The office action further states, " As to claim 22, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56).*

In response applicant respectfully states that Claim 22 employs pair-wise differentially uniform numbers as in claim 3, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 22, which is dependent on Claim 3, is allowable over Furuya et al.

> *The office action further states, " As to claim 23, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).*

In response applicant respectfully states that Claim 23 employs pair-wise differentially uniform numbers as in claim 11, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 23, which is dependent on Claim 11, is allowable over Furuya et al.

The office action further states, " As to claim 26, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 1 above).

In response applicant respectfully states that Claim 26 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 26, which is dependent on Claim 1, is allowable over Furuya et al.

The office action further states, " As to claim 28, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 1 above).

In response applicant respectfully states that Claim 28 is dependent on Claim 1.

The office action further states, " As to claim 30, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 1 (see Furuya et al., page 2, lines 3-5).

In response applicant respectfully states that Claim 30 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 30, which is dependent on Claim 1, is allowable over Furuya et al.

The office action further states, " As to claim 33, Furuya et al. teaches an apparatus to encrypt a plain-text message (see page 2, lines 1-3), the apparatus comprising: a Pairwise Additively Uniform Sequence Generator to further expand a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 5, line 54 through page 8, line 10); an Encryptor to divide said plain-text message into a plurality of plain-text blocks (see figure 15), and to encrypt said plain-text blocks to form a plurality of cipher-text blocks (see page 5, lines 31-38); a Checksum Generator to combine said plurality of plain-text blocks into at least one check sum (see figure 6); and an Integrity Extractor and Checker to employ said set of pair-wise differentially- uniform pseudo random *numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks (see page 5, lines 39-43). Furuya et al. does not teach a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number. Takahashi teaches a Randomness Generator to generate a first random number (see column 3, lines 4-13); and a Randomness Transformer to transform said first random number into a first pseudo random number (see column 3, lines 14-29). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Takahashi because a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20).*

In response applicant respectfully states that the phrase in claim 33, "Pairwise Additively Uniform Sequence Generator" has the same meaning as a " Pairwise Differentially Uniform Sequence Generator". Thus Claim 33 employs pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., with Takahashi do not teach generating or employing pair-wise additively uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 33, is allowable over Furuya et al.

The office action further states, " As to claim 35, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a Computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).

In response applicant respectfully states that Claim 35 employs pair-wise differentially uniform numbers as in claim 2, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 35, which is dependent on Claim 2, is allowable over Furuya et al.

The office action further states, " As to claim 37, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means

> *for causing a computer to effect the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).*

In response applicant respectfully states that Claim 37 employs pair-wise differentially uniform numbers as in claim 2, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 37, which is dependent on Claim 2, is allowable over Furuya et al.

> *The office action further states, " As to claim 39, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).*

In response applicant respectfully states that Claim 39 employs pair-wise differentially uniform numbers as in claim 2, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 39, which is dependent on Claim 2, is allowable over Furuya et al.

> *The office action further states, " As to claim 41, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., figure 15).*

In response applicant respectfully states that Claim 41 employs pair-wise differentially uniform numbers as in claim 3, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 41, which is dependent on Claim 3, is allowable over Furuya et al.

> *The office action further states, " As to claim 42, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., figure 15).*

In response applicant respectfully states that Claim 42 employs pair-wise differentially uniform numbers as in claim 11, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 42, which is dependent on Claim 11, is allowable over Furuya et al., combined with Takahashi.

> *The office action further states, " 10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063811 A 1) in view of Takahashi (U.S. patent No. 5,570,307) as applied to claims 1-6,8,10-12,22-23,26,28,30,33,35, 37,39, and 41-42 above. and further in view of Cane et al., (U.S. patent No. 5,940,507).*

> *As to Claim 7, Furuya et al. as modified, still does not teach wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks. Cane et at. teaches wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks (see column 4, lines 4-15). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).*

In response applicant respectfully states that Claim 7 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 37, which is dependent on Claim 1, is allowable over Furuya et al. with or without Takahashi and Cane et al.

> *The office action further states, " 11. Claim 9 is rejected under 35 U.S.C. 103 (a) as being unpatentable over Furuya et & (European patent application publication No.1 063811 A1) in view of Takahashi (U.S. patent No. 5,570,307) as applied to claims 1-6,8,10-12,22-23,26,28,30,33,35, 37, 39, and 41-42 above, and further in view of Hardy et al. (U.S. patent No.5, 195, 136).*

> *As to Claim 9, Furuya et al. as modified, still does not teach wherein the step of transforming said random number includes a cryptographic operation. Hardy et al. teaches wherein the step of transforming said random number includes a cryptographic operation (see column 4, line 67 through column 5, line 21). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of transforming said random number includes a cryptographic operation.*

> *It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Hardy et al. because wherein the step of transforming said random number includes a cryptographic operation would produce a traffic key that could be added to a text bit stream to produce cipher text (see Hardy et al., column 5, lines 10-21).*

In response applicant respectfully states that Claim 9 employs pair-wise differentially uniform numbers as in claim 1, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 9, which is dependent on Claim 1, is allowable over Furuya et al. with or without Takahashi and Hardy et al.

The office action further states, " 12. Claims 13-15, 18-21, 24-25, 27, 29, 31, 34, 36, 38, 40, 43-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No.1 063811 A1) in view of Brandman (U.S. patent No. 5,974,144)".

As to Claim 13, Furuya et al. teaches a method for decrypting a cipher-text message (see page 2, lines 3-5), the method comprising: dividing said cipher-text message into a plurality of cipher-text blocks (see page 7, lines 43-47); decrypting said cipher-text blocks in forming a plurality of plain-text blocks (see page 7, lines 43-50); further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21); combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to form a plurality of output blocks (see page 7, lines 48-50); and comparing said at least two check sums in declaring success of a message integrity check (see page 5, lines 25-26 and see lines 39-43).

Furuya et al. does not teach transforming at least one of said plain-text blocks into a first pseudo random number. Brandman teaches transforming at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include transforming at least one of said plain-text blocks into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Brandman because transforming at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).

In response applicant respectfully states that claim 13 includes, "further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers." Furuya et al. and Brandman do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 13, is allowable over Furuya et al. with or without Brandman.

The office action further states, " As to claim 14, Furuya et al. as modified, teaches wherein the step of decrypting said cipher-text blocks includes employing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers (see Furuya et al., page 7, lines 43-50).

In response applicant respectfully states that Furuya et al, with Brandman do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 14, which is dependent on Claim 13, is allowable over Furuya et al. with or without Brandman.

> *The office action further states, " As to claim 15, Furuya et al. as modified, teaches wherein the step of combining includes: pairing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks (see Furuya et al., figure 8); and using each pair to form a plurality of output blocks and employing the output blocks to form said at least two check sums (see Furuya et al., page 5, lines 25-26, and see lines 39-43).*

In response applicant respectfully states that claim 15 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 16, which is dependent on Claim 13, is allowable over Furuya et al., and Brandman

> *The office action further states, " As to claim 18, Furuya et al. as modified, teaches wherein the step of transforming said plain-text blocks includes a non-cryptographic or linear operation (see Brandman, figure 3).*

In response applicant respectfully states that Claim 18 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 16, which is dependent on Claim 13, is allowable over Furuya et al., and Brandman

> *The office action further states, " As to Claim 19, Furuya et al. as modified, teaches wherein the step of transforming said plain-text blocks includes a cryptographic operation (see Brandman, column 5, lines 6-34).*

In response applicant respectfully states that Claim 19 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 19, which is dependent on Claim 13, is allowable over Furuya et al., and Brandman

> *The office action further states, " As to Claim 20, Furuya et al. as modified, teaches wherein the said set of pair- wise differentially-uniform numbers are set of pair-wise*

> *differentially-uniform numbers in GFp (see Furuya et al., page 7, line 54 through page 8, line 10).*

In response applicant respectfully states that claim 20 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Although Furuya et al., may teach using operations in GFp, it does not teach generating or using numbers which are pairwise differentially uniform in GFp. Thus claim 20, which is dependent on Claim 13, is allowable over Furuya et al.

> *The office action further states, "As to Claim 21, Furuya et al. as modified, teaches wherein the step of employing includes: pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and combining each pair to form a plurality of input blocks used in said step of decrypting (see Furuya et al., page 7, lines 43-50).*

In response applicant respectfully states that claim 21 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., does not teach employing pair-wise differentially uniform numbers. Thus claim 21, which is dependent on Claim 14, is allowable over Furuya et al.

> *The office action further states, "As to Claim 24, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).*

In response applicant respectfully states that Claim 24 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., does not teach employing pair-wise differentially uniform numbers. Thus claim 24, which is dependent on Claim 15, is allowable over Furuya et al.

> *The office action further states, "As to claim 25, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).*

In response applicant respectfully states that Claim 25 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., does not teach employing pair-wise differentially uniform numbers. Thus claim 25, which is dependent on Claim 21, is allowable over Furuya et al.

> *The office action further states, " As to Claim 27, Furuya- et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).*

In response applicant respectfully states that Claim 27 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 27, which is dependent on Claim 13, is allowable over Furuya et al.

> *The office action further states, " As to Claim 29, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).*

In response applicant respectfully states that Claim 29 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 29, which is dependent on Claim 13, is allowable over Furuya et al.

> *The office action further states, " As to Claim 31, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).*

In response applicant respectfully states that claim 31 employs pair-wise differentially uniform numbers as in claim 13, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 31, which is dependent on Claim 13, is allowable over Furuya et al.

> *The office action further states, " As to Claim 34, Furuya et al. teaches an apparatus to decrypt a cipher-text message (see page 2, lines 3-5), the apparatus comprising: a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks (see page 7, lines 43-47), and to decrypt said cipher-text blocks in forming a plurality of plain-text blocks (see page 7, lines 43-50); a Pairwise Additively Uniform Sequence Generator to further expand at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21); a Checksum Generator to combine said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to form a plurality of output blocks (see page 7, lines 48-50); and an Integrity Extractor and Checker to compare said at least two check sums in declaring success of a message integrity check (see column 5, lines 25-26 and see lines 39-43). Furuya et al. does not teach a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number. Brandman teaches a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Brandman because a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).*

In response applicant respectfully states that claim 34, has a "Pairwise Additively Uniform Sequence Generator. A Pairwise Additively Uniform Sequence Generator has the same meaning as a " Pairwise Differentially Uniform Sequence Generator". Thus Claim 34 employs pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., with Takahashi do not teach generating or employing pair-wise additively uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 34, is allowable over Furuya et al., with Takahashi.

> *The office action further states, " As to Claim 36, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a Computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 14 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).*

In response applicant respectfully states that claim 36 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 36, which is dependent on Claim 14, is allowable over Furuya et al.

> *The office action further states, " As to Claim 38, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 14 (for the teachings of this .claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).*

In response applicant respectfully states that Claim 38 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 38, which is dependent on Claim 14, is allowable over Furuya et al.

> *The office action further states, "As to Claim 40, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 14 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).*

In response applicant respectfully states that Claim 40 employs pair-wise differentially uniform numbers as in claim 14, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 40, which is dependent on Claim 14, is allowable over Furuya et al.

> *The office action further states, " As to Claim 43, Furuya et al. as modified, teaches wherein the step of using each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., page 7, lines 43-50).*

In response applicant respectfully states that Claim 43 employs pair-wise differentially uniform numbers as in claim 15, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 43, which is dependent on Claim 15, is allowable over Furuya et al.

> *The office action further states, " As to Claim 44, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., page 7, lines 43-50).*

In response applicant respectfully states that Claim 44 employs pair-wise differentially uniform numbers as in claim 21, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 44, which is dependent on Claim 21, is allowable over Furuya et al.

> *The office action further states, " As to Claim 45, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., page 7, lines 43-50).*

In response applicant respectfully states that Claim 45 employs pair-wise differentially uniform numbers as in claim 21, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 45, which is dependent on Claim 21, is allowable over Furuya et al.

> *The office action further states, " 13. Claim 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No.1 063 811 A 1) in view of Brandman (U.S. patent No. 5,974,144) as applied to claims 13-15,18-21,24-25,27,29, 31,34, 36, 38,40,43-45 above: and further in view of Cane et al., (U.S. patent No. 5,940,507).*
>
> *As to Claim 16, Furuya et al. as modified, still does not teach wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair. Cane et al. teaches wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair (see column 4, lines 4-15). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya at al. as modified, to include wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).*

In response applicant respectfully states that claim 16 employs pair-wise differentially uniform numbers as in claim 15, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., with Cane do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 44, which is dependent on Claim 21, is allowable over Furuya et al., and Cane.

> *The office action further states, " As to Claim 17, Furuya et al. as modified, still does not teach wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an exclusive-or of said subsets of output blocks. . Cane et al. teaches wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an exclusive-or of said subsets of output blocks (see column 4, lines 4-15). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an exclusive-or of said subsets of output blocks. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an exclusive-or of said subsets of output blocks would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).*

In response applicant respectfully states that Claim 17 employs pair-wise differentially uniform numbers as in claim 15, which are much weaker and easier to generate than general purpose pseudo random numbers. Furuya et al., with Cane et al., do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. Thus claim 17, which is dependent on Claim 15, is allowable over Furuya et al., with Cane.

> *The office action further states, " 14. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A 1) in view of Takahashi (U.S. patent No. 5,570,307), and further in view of Brandman (U.S. patent No. 5,974,144).*
>
> *As to Claim 32, Furuya et al. teaches a method for encryption/decryption of a plain-text message (see page 2, lines 1-3), the method comprising the steps of: further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 7, line 54 through page 8, line 10); dividing the plain-text message into a plurality of plain-text blocks (see figure 15); encrypting said plain-text blocks in forming a plurality of cipher-text blocks (see page 5, lines 31-38); combining said plurality of plain-text blocks into at least one check sum (see figure 6); and employing said first random number, said first pseudo random number and said set of pair-wise*

differentially-uniform pseudo random numbers to embed a message integrity check in said cipher-text blocks to form a cipher-text message (see page 5, lines 39-43); and dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of said plain-text message; - decrypting said cipher-text blocks in forming a plurality of plain-text blocks (see . page 7, lines 43-50); further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21); combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block. to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to re- form the said plain-text message (see page 7, lines 48-50); and comparing said at least two check sums in declaring success of a message integrity check in decryption of said cipher-text to reform said plain-text message (see page 5, lines 25-26 and see lines 39-43). Furuya et al. does not teach generating a first random number; and transforming said first random number into a first pseudo random number. Takahashi teaches generating a first random number (see column 3, lines 4-13); and transforming said first random number into a first pseudo random number (see column 3, lines 14-29). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include generating a first random number; and transforming said first random number into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuva et al. by the teachings of Takahashi because generating a first random number; and transforming said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20). Furuva et al. as modified, still does not teach transforming at least one of said plain-text blocks into a first pseudo random number. Brandman teaches transforming at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuva et al. as modified, to include transforming at least one of said plain-text blocks into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Brandman because transforming at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).

In response applicant respectfully states that Claim 32 includes, "further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers." Furuya et al., with Brandman do not teach employing pair-wise differentially uniform numbers, which are much weaker and easier to generate than general purpose pseudo random numbers. In Figure 21 of Furuya et al.,, they teach generating general purpose pseudo random numbers, called the key stream S(i), which is much more expensive than generating a sequence of numbers, say S'(i), which are only pairwise differentially uniform random. It is not at all obvious how such a weaker sequence of pair-wise differentially-uniform pseudo random numbers can be employed to assure encryption and integrity. The present invention of using pair-wise differentially-uniform pseudo random numbers has unexpected results described in the specification, [cheaper to generate, etc.] which are indeed not obvious. The encryption scheme of claim 32, generates a cipher-text with message integrity with little additional computational cost, while retaining at least the same level of security as schemes based on a MAC. Thus claim 32, is allowable over Furuya et al., with Brandman.

Furthermore, applicant does not agree with many of the statements and allegations made in the office action regarding the claims in the present invention and regarding the cited references, and asks the Examiner to provide support for these. However, in light of the clear novelty, advantages, non-obviousness and unexpected results of the invention in claim 1-47, there is no need to provide arguments in this regard.

In conclusion claims 1-47 are allowable over the cited references. Applicants invention as originally claimed and corrected herein is novel and non-obvious over the cited art. It is anticipated that this amendment brings the application to allowance of claims 1-47, and favorable action is respectfully solicited. In the unlikely event that any claim remains rejected, please contact the undersigned by phone in order to discuss the application.

Please charge any fee necessary to enter this paper to deposit account 09-0458.

Respectfully submitted,

By: Louis Herzberg
Dr. Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (914) 945-2885
Fax. (914) 945-3281

IBM CORPORATION
Intellectual Property Law Dept.
P.O. Box 218
Yorktown Heights, New York 10598